
# 401 – MSN SESSION LOGS AND CHAT

## TEAM INFORMATION

**Team Name:** _____

**Results Email:** _____

**Examination Time Frame:** _____ to _____

## INSTRUCTIONS

**Description**: Examiners must develop and document a methodology used to parse MSN Session Logs and Chat communications from the presented MSN Chat program files contained in the folder **401_MSN_Session_Logs_and_Chat_Challenge2008** to an easily understandable and readable format. The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

**Total Weighted Points**: **80 Total Points available per entry – Total 400 Points Available**

1. **Answers –** Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

## INTERNAL REVIEWER USE ONLY

| | | | |
|---|---|---|---|
| Reviewer: | | Points Awarded: | |
| Date: | | Review Period: | to |
| Completed: | ☐ Yes ☐ No ☐ Partial | | |

**<Example Area>**

User Logon Name (Date/Time if Available) Conversation
Additional Information As Available

User Logon Name (Date/Time if Available) Conversation
Additional Information As Available

User Logon Name (Date/Time if Available) Conversation
Additional Information As Available

**<Answer Area>**

Methodology and noted information for process:

User Logon Name (Date/Time if Available) Conversation
Additional Information As Available

Please attach additional sheets as needed.

# METHODOLOGY / NOTES FORM

## Tool Information

| Type | Name | Publisher |
|---|---|---|
| Commercial / Open Source | | |

**Site:**

| Type | Name | Publisher |
|---|---|---|
| Commercial / Open Source | | |

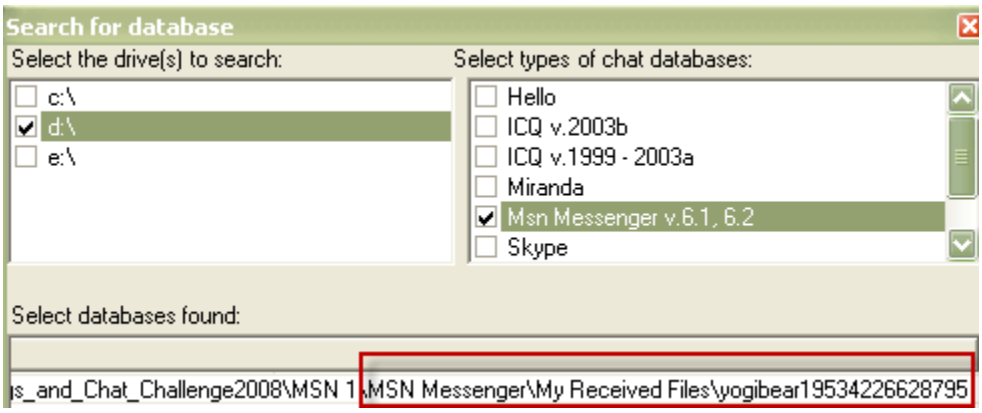
**Site:**

| Type | Name | Publisher |
|---|---|---|
| Commercial / Open Source | | |

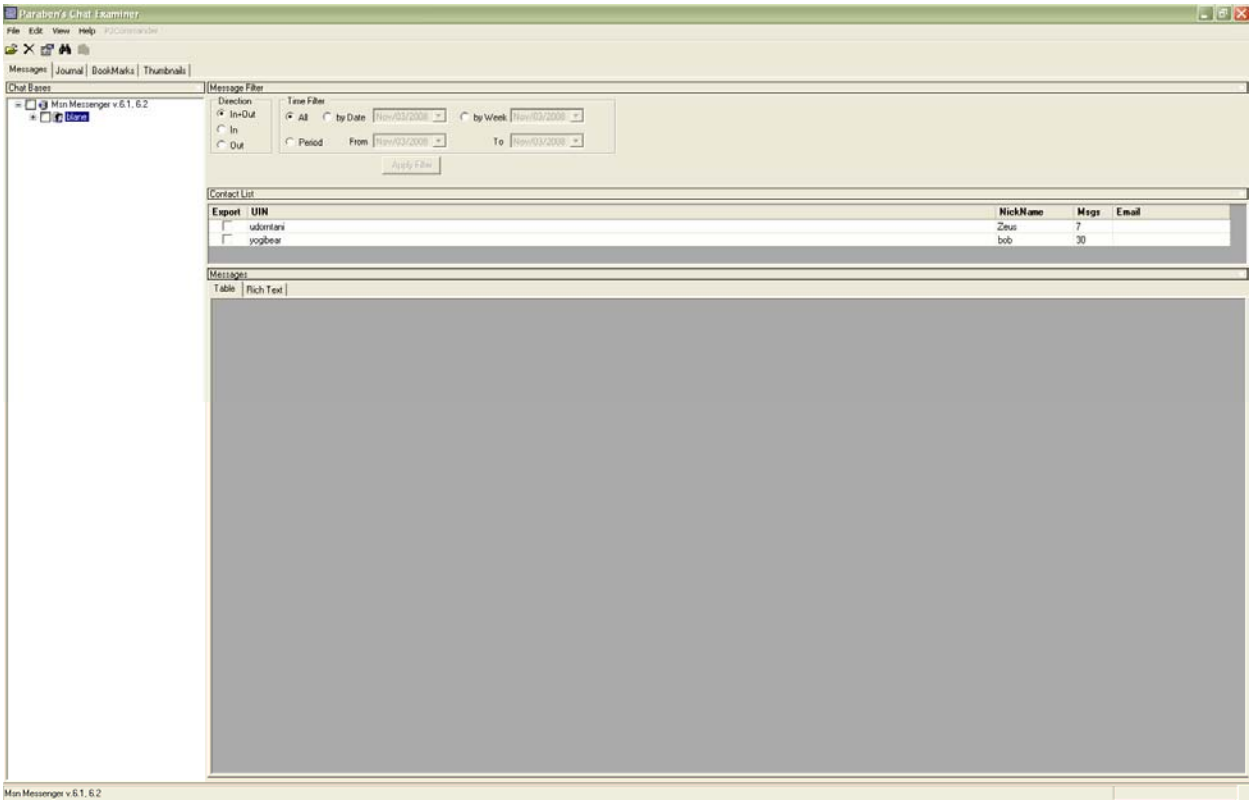
**Site:**

| Date/Time | Notes |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

1) To parse the log files i used Paraben's Chat Examiner (http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=162)
2) I selected the 401-MSN Session Logs and Chat challenge section of the DVD. AS seen in the screenshot below, the software application found a MSN chat database.

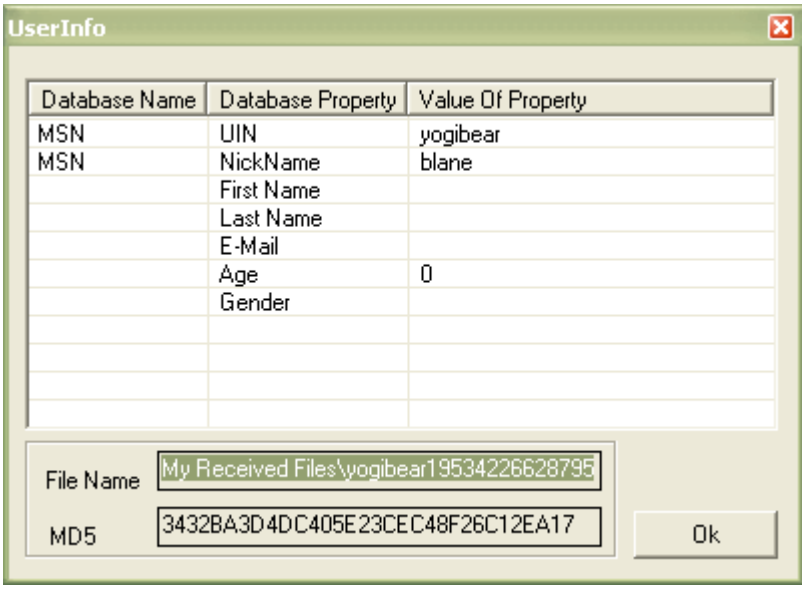



3) Below is a screenshot of the chat database loaded into the software



As you can see in the above screenshot, there are two accounts with chat logs. The UIN "udorntani" with the NickName "Zeus" and UIN "yogibear" with the NickName "bob. As seen in the upper right hand corner of the above screenshot, you see the nickname

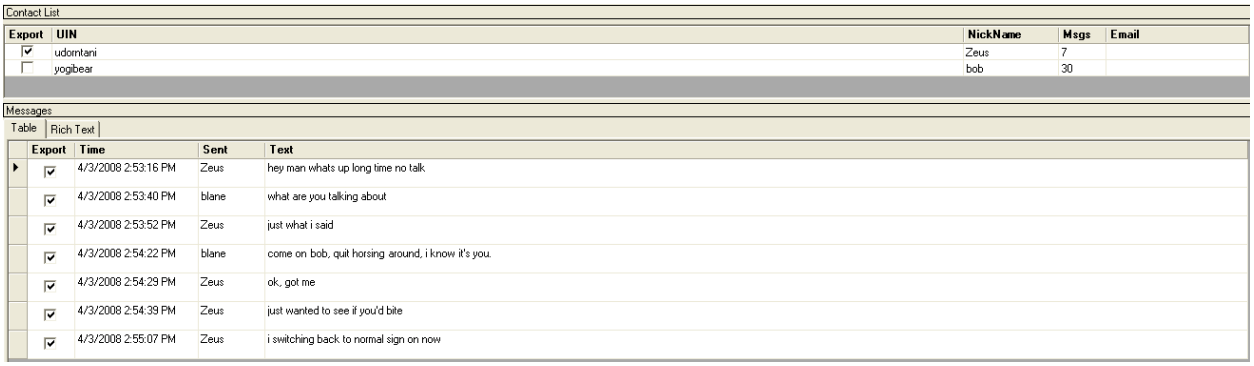
"Blane" which has the following UIN "yogibear". See below for supporting information. This finding is consistent with the UIN "yogibear" having two nicknames – "bob" and "blane".




4) Below are the chat logs from "Zeus" to "Blane"

Zeus 4/3/2008 2:53:16 PM : hey man whats up long time no talk
blane 4/3/2008 2:53:40 PM : what are you talking about
Zeus 4/3/2008 2:53:52 PM : just what i said
blane 4/3/2008 2:54:22 PM : come on bob, quit horsing around, i know it's you.
Zeus 4/3/2008 2:54:29 PM : ok, got me
Zeus 4/3/2008 2:54:39 PM : just wanted to see if you'd bite
Zeus 4/3/2008 2:55:07 PM : i switching back to normal sign on now

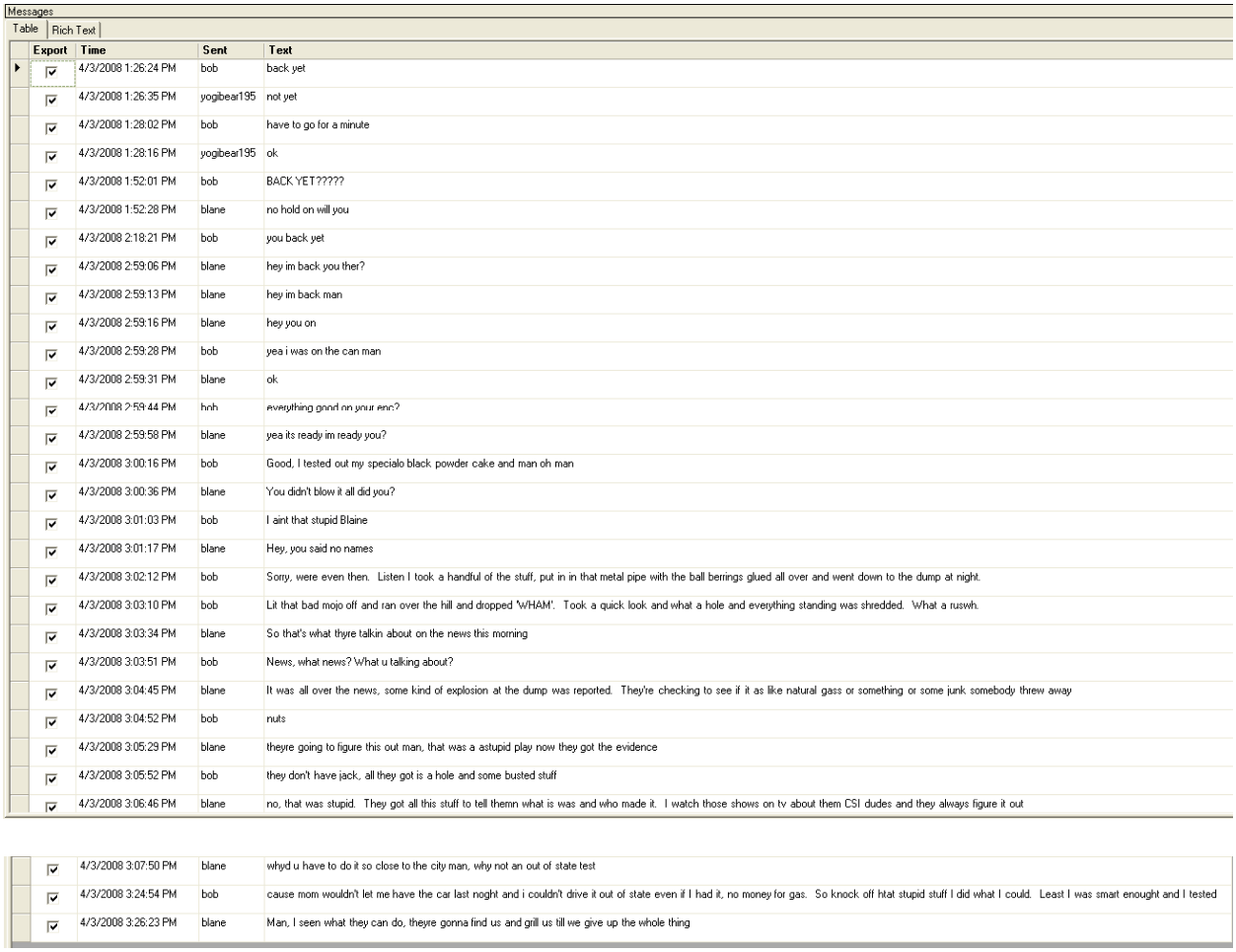
Below is a screenshot




5) Below are the chat logs from "bob" "blane" and "yogibear1953@hotmail.com"

bob 4/3/2008 1:26:24 PM : back yet
yogibear1953@hotmail.com 4/3/2008 1:26:35 PM : not yet
bob 4/3/2008 1:28:02 PM : have to go for a minute
yogibear1953@hotmail.com 4/3/2008 1:28:16 PM : ok
bob 4/3/2008 1:52:01 PM : BACK YET?????
blane 4/3/2008 1:52:28 PM : no hold on will you
bob 4/3/2008 2:18:21 PM : you back yet
blane 4/3/2008 2:59:06 PM : hey im back you ther?
blane 4/3/2008 2:59:13 PM : hey im back man
blane 4/3/2008 2:59:16 PM : hey you on
bob 4/3/2008 2:59:28 PM : yea i was on the can man
blane 4/3/2008 2:59:31 PM : ok
bob 4/3/2008 2:59:44 PM : everything good on your enc?
blane 4/3/2008 2:59:58 PM : yea its ready im ready you?
bob 4/3/2008 3:00:16 PM : Good, I tested out my specialo black powder cake and man oh man
blane 4/3/2008 3:00:36 PM : You didn't blow it all did you?
bob 4/3/2008 3:01:03 PM : I aint that stupid Blaine
blane 4/3/2008 3:01:17 PM : Hey, you said no names
bob 4/3/2008 3:02:12 PM : Sorry, were even then. Listen I took a handful of the stuff, put in in that metal pipe with the ball berrings glued all over and went down to the dump at night.
bob 4/3/2008 3:03:10 PM : Lit that bad mojo off and ran over the hill and dropped 'WHAM'. Took a quick look and what a hole and everything standing was shredded. What a ruswh.
blane 4/3/2008 3:03:34 PM : So that's what thyre talkin about on the news this morning
bob 4/3/2008 3:03:51 PM : News, what news? What u talking about?
blane 4/3/2008 3:04:45 PM : It was all over the news, some kind of explosion at the dump was reported. They're checking to see if it as like natural gass or something or some junk somebody threw away
bob 4/3/2008 3:04:52 PM : nuts
blane 4/3/2008 3:05:29 PM : theyre going to figure this out man, that was a astupid play now they got the evidence
bob 4/3/2008 3:05:52 PM : they don't have jack, all they got is a hole and some busted stuff
blane 4/3/2008 3:06:46 PM : no, that was stupid. They got all this stuff to tell themn what is was and who made it. I watch those shows on tv about them CSI dudes and they always figure it out
blane 4/3/2008 3:07:50 PM : whyd u have to do it so close to the city man, why not an out of state test
bob 4/3/2008 3:24:54 PM : cause mom wouldn't let me have the car last noght and i couldn't drive it out of state even if I had it, no money for gas. So knock off htat stupid stuff I did what I could. Least I was smart enought and I tested it out and those tv shors are just that and a bunch of stuff too.
blane 4/3/2008 3:26:23 PM : Man, I seen what they can do, theyre gonna find us and grill us till we give up the whole thing

Below is a screenshot from the program



Messages

Table | Rich Text

| Export | Time | Sent | Text |
|---|---|---|---|
| ☑ | 4/3/2008 1:26:24 PM | bob | back yet |
| ☑ | 4/3/2008 1:26:35 PM | yogibear195 | not yet |
| ☑ | 4/3/2008 1:28:02 PM | bob | have to go for a minute |
| ☑ | 4/3/2008 1:28:16 PM | yogibear195 | ok |
| ☑ | 4/3/2008 1:52:01 PM | bob | BACK YET????? |
| ☑ | 4/3/2008 1:52:28 PM | blane | no hold on will you |
| ☑ | 4/3/2008 2:18:21 PM | bob | you back yet |
| ☑ | 4/3/2008 2:59:06 PM | blane | hey im back you ther? |
| ☑ | 4/3/2008 2:59:13 PM | blane | hey im back man |
| ☑ | 4/3/2008 2:59:16 PM | blane | hey you on |
| ☑ | 4/3/2008 2:59:28 PM | bob | yea i was on the can man |
| ☑ | 4/3/2008 2:59:31 PM | blane | ok |
| ☑ | 4/3/2008 2:59:44 PM | bob | everything good on your end? |
| ☑ | 4/3/2008 2:59:58 PM | blane | yea its ready im ready you? |
| ☑ | 4/3/2008 3:00:16 PM | bob | Good, I tested out my specialo black powder cake and man oh man |
| ☑ | 4/3/2008 3:00:36 PM | blane | You didn't blow it all did you? |
| ☑ | 4/3/2008 3:01:03 PM | bob | I aint that stupid Blaine |
| ☑ | 4/3/2008 3:01:17 PM | blane | Hey, you said no names |
| ☑ | 4/3/2008 3:02:12 PM | bob | Sorry, were even then. Listen I took a handful of the stuff, put in in that metal pipe with the ball berrings glued all over and went down to the dump at night. |
| ☑ | 4/3/2008 3:03:10 PM | bob | Lit that bad mojo off and ran over the hill and dropped 'WHAM'. Took a quick look and what a hole and everything standing was shredded. What a ruswh. |
| ☑ | 4/3/2008 3:03:34 PM | blane | So that's what thyre talkin about on the news this morning |
| ☑ | 4/3/2008 3:03:51 PM | bob | News, what news? What u talking about? |
| ☑ | 4/3/2008 3:04:45 PM | blane | It was all over the news, some kind of explosion at the dump was reported. They're checking to see if it as like natural gass or something or some junk somebody threw away |
| ☑ | 4/3/2008 3:04:52 PM | bob | nuts |
| ☑ | 4/3/2008 3:05:29 PM | blane | theyre going to figure this out man, that was a astupid play now they got the evidence |
| ☑ | 4/3/2008 3:05:52 PM | bob | they don't have jack, all they got is a hole and some busted stuff |
| ☑ | 4/3/2008 3:06:46 PM | blane | no, that was stupid. They got all this stuff to tell themn what is was and who made it. I watch those shows on tv about them CSI dudes and they always figure it out |
| ☑ | 4/3/2008 3:07:50 PM | blane | whyd u have to do it so close to the city man, why not an out of state test |
| ☑ | 4/3/2008 3:24:54 PM | bob | cause mom wouldn't let me have the car last noght and i couldn't drive it out of state even if I had it, no money for gas. So knock off htat stupid stuff I did what I could. Least I was smart enought and I tested |
| ☑ | 4/3/2008 3:26:23 PM | blane | Man, I seen what they can do, theyre gonna find us and grill us till we give up the whole thing |